CLAIMS

1. A method for utilizing a public wireless local area network for a client with a smart card, comprising:

creating a password for a client;

storing the password and identification information of the client on a public wireless local area network; and

utilizing the password and the client identity information to authenticate the client in the public wireless local area network.

2. The method of claim 1 wherein the authentication is provided by a Remote Authentication Dial-In User Service (RADIUS) server.

3. The method of claim 1 further comprising authenticating the client by a second server based on a smart card.

4. The method of claim 1 further comprising authenticating the client by a second server based on a universal subscriber identity module card.

5. The method of claim 1 further comprising authenticating the client by a second server based on a subscriber identity module card.

6. The method of claim 1 further comprising modifying accounting data from the public wireless local area network to include charging data record fields for the client.

7. The method of claim 1 wherein the creating is independently performed by each of two entities.

8. The method of claim 1 wherein the creating comprises utilizing international mobile subscriber identity (IMSI) of the client.

9. The method of claim 1 wherein the creating comprises utilizing a pseudonym of the client.

10. The method of claim 1 wherein the creating comprises utilizing MicroSoft - Microsoft Point-to-Point Encryption (MS-MPPE)-Send-Key.

11. The method of claim 1 wherein the creating comprises utilizing MicroSoft - Microsoft Point-to-Point Encryption (MS-MPPE)-Recv-Key.

12. The method of claim 1 wherein the creating comprises calculating a hash value.

13. The method of claim 1 wherein the creating comprises calculating a hash value using a SHA-1 hashing process.

14. A system for utilizing a public wireless local area network for a client with a smart card, comprising:

a smart card for a client; and

a first adapter for generating a password for the client, wherein the password is used for authenticating the client by a Remote Authentication Dial-In User Service (RADIUS) server.

15. The system of claim 14 further comprising a second adapter for authenticating the client by a second server based on the smart card.

16. The system of claim 14 wherein the first and second adapters reside on separate devices.

17. The system of claim 15 further comprising a third adapter for modifying RADIUS based accounting data to generate General Packed Radio Server (GPRS) based accounting data.

18. The system of claim 14 further comprising a fourth adapter for generating the password for the client.

19. A method for adapting a public wireless local area network for a client with a smart card, comprising:

creating a password for a client based on identification information of the client;

storing the password and the identification information on a Remote Authentication Dial-In User Service (RADIUS) server;

utilizing the password and the identification information to authenticate the client on the RADIUS server; and

modifying RADIUS based accounting data to generate General Packed Radio Server (GPRS) based accounting data for the client.

20. The method of claim 19 wherein the creating comprises deriving the following: password = F (generating a hash value (Username | n*Value | "sim direct")), wherein Username comprises the identification information of the client, wherein Value is selected from the group consisting of: Kc, which is a 64 bit ciphering key known in the art; MicroSoft - Microsoft Point-to-Point Encryption (MS-MPPE)-Send-Key; and MS-MPPE-Recv-Key, wherein F is a function for converting a hash value into an alpha-numeric string.